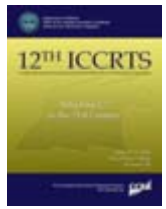
Game Theoretic Solutions to Cyber Attack and Network Defense Problems

12th ICCRTS

"Adapting C2 to the 21st Century"

Newport, Rhode Island, June 19-21, 2007



Twelfth International Command and Control Research and Technology Symposium

Intelligent Automation, Inc
Dan Shen, Genshe Chen

Cruz & Associates
J. B. Cruz, Jr.

AFRL/SNAA
Erik Blasch

The Office of Naval Research
Martin Kruger

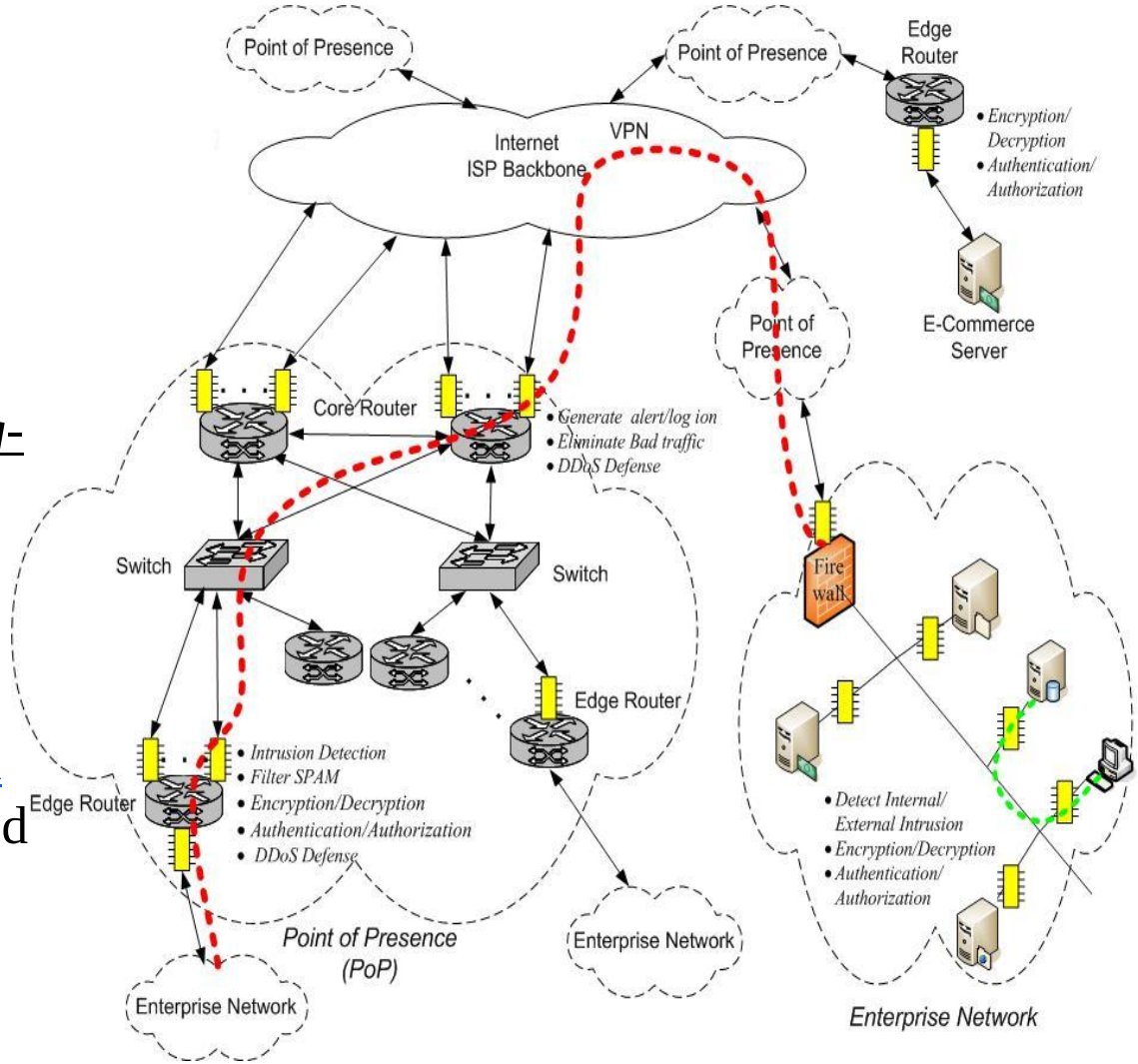
Outline

- Introduction
- Overall Framework
- Markov Game model for Cyber Network Defense
- Simulations and Experiments
- Conclusions

Introduction to the Problem

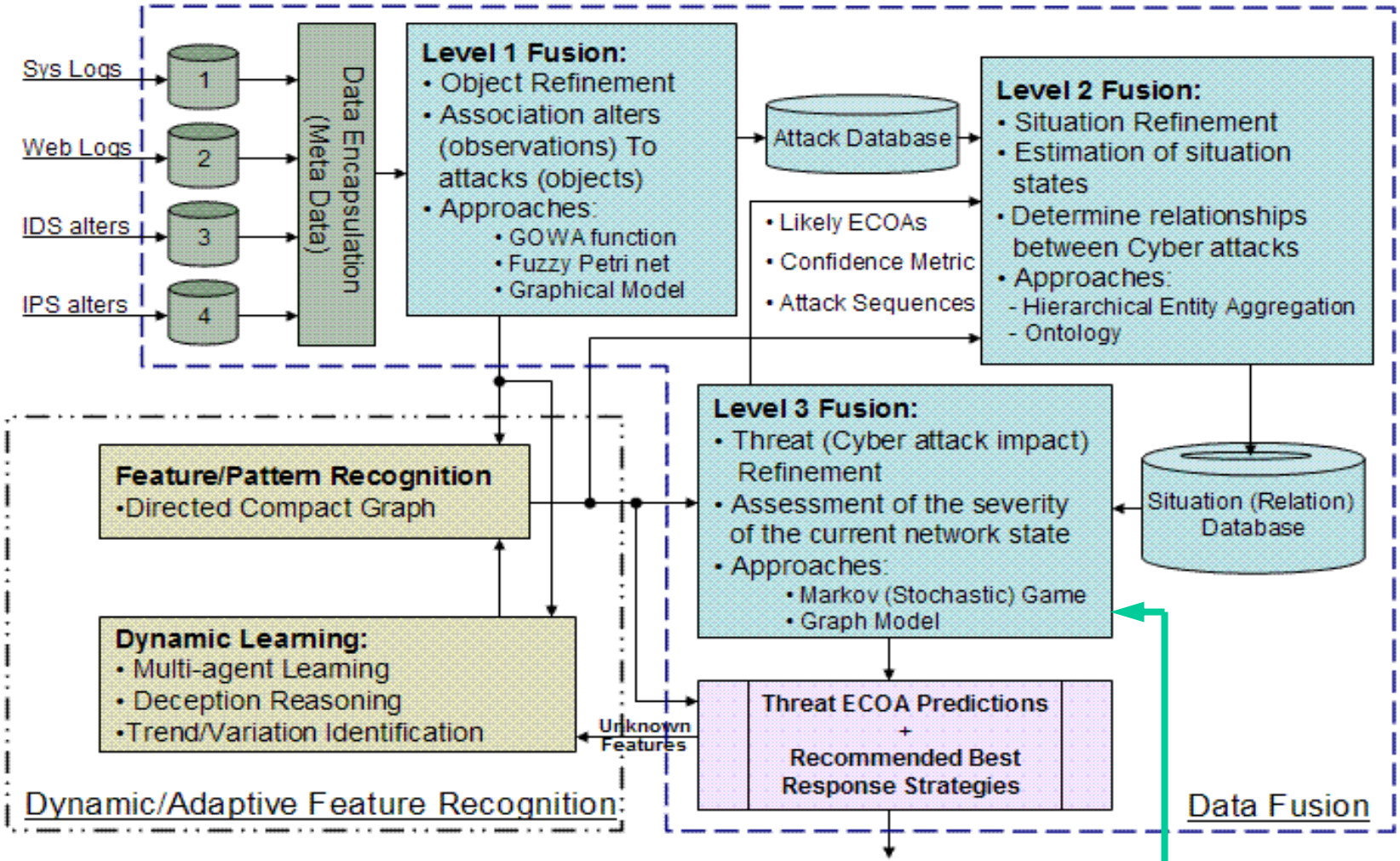
Intelligent Automation, Inc.

- The cyberspace security requires next-generation network management and intrusion detection systems.
- These systems should combine both *short-term sensor information* and *long-term knowledge databases.* to provide decision-support and cyberspace command and control.
- We propose an information fusion and data mining based decision and control framework to detect and predict the multistage stealthy cyber attacks.



System Architecture

Intelligent Automation, Inc.



The focus of this paper

Key Components

- Similar to the battle-space architecture, our cyberspace security system has two fully coupled major parts:
  - Data fusion module (to refine primitive awareness and assessment; to identify new cyber attacks);
  - Dynamic/adaptive feature recognition module (to generate primitive estimations; to learn new identified new or unknown cyber attacks).
- Various logs and Intrusion Detection Sensors (IDS) alerts are fed into the L1 data fusion components.
- The fused objects and related pedigree information are used by a <u>feature/pattern recognition module</u> to generate primitive prediction of intents of cyber attackers.
- High-level (L2 and L3) data fusion based on Markov game model is proposed to refine the primitive prediction
- The captured unknown/new cyber attack patterns will be associated to related L1 results in dynamic learning block,

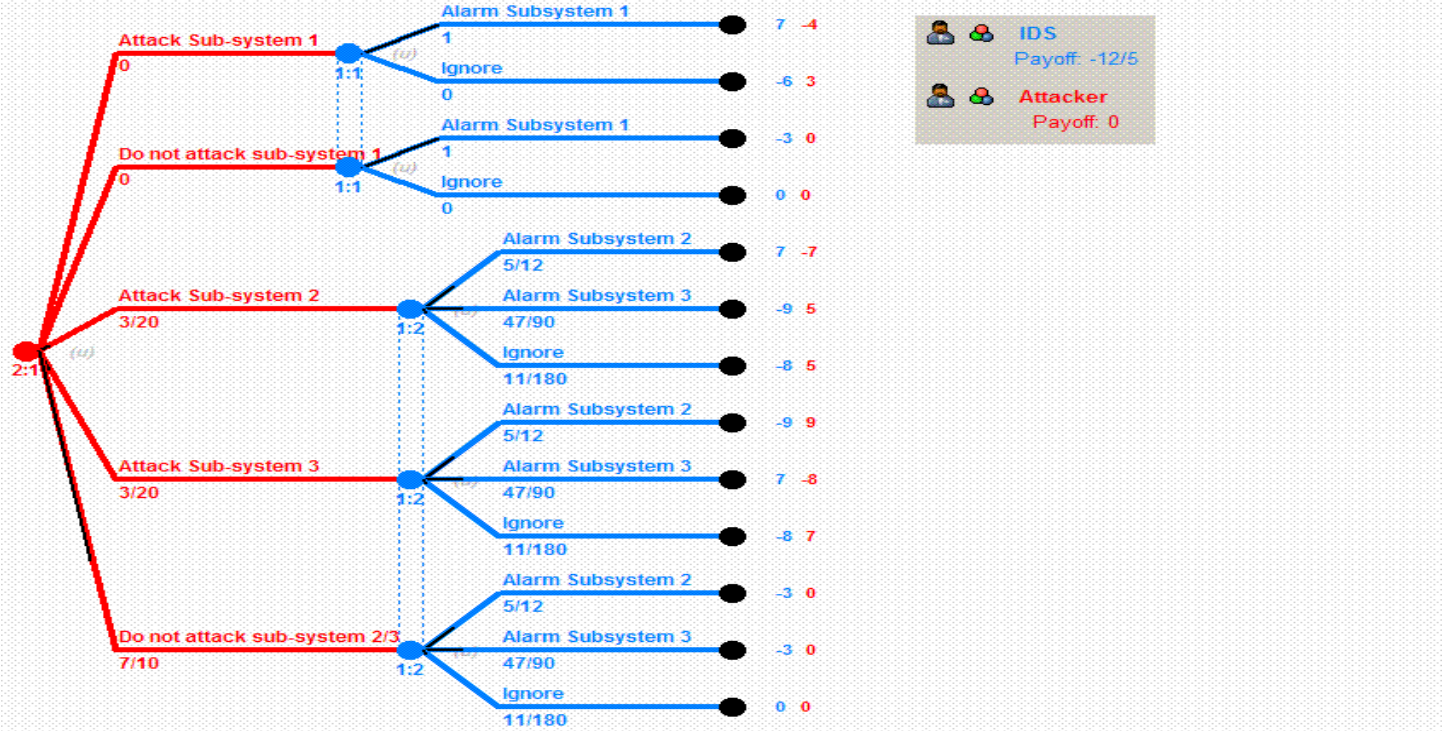
Key Features

- Recognition/Refinement/Learning Structure --- Data mining
- A Decentralized multiplayer non-zero sum Markov Game Model
  - Markov (Stochastic) game model is used to estimate the belief of each possible Enemy Course of Action (ECOA).
  - The actions of white objects are modeled as the *third player* in the non-zero sum Markov game framework.
- A Hierarchical Entity Aggregation
  - Lower level entity (node) aggregation --- clique-based clustering protocol and Fair and Secure Clustering Scheme (FSCS) clustering protocol
  - High level entity (node) aggregation --- a collection of entities collaborating to achieve the *same tactical goal.*
- Ontology
- EWMA (Exponentially Weighted Moving Average)

Game Theoretic Approaches -- Review

Intelligent Automation, Inc.

- Current game theoretic approaches[1-2] for cyber network intrusion detection and decision support are based on static matrix games



1: Attack Sub-system 1	1: Do not attack sub-system 1	1: Attack Sub-system 2	1: Attack Sub-system 3	1: Do not attack sub-system 2/3
0	0	$\frac{3}{20}$	$\frac{3}{20}$	$\frac{7}{10}$

1: Alarm Subsystem 1	1: Ignore	2: Alarm Subsystem 2	2: Alarm Subsystem 3	2: Ignore
1	0	$\frac{5}{12}$	$\frac{47}{90}$	$\frac{11}{180}$

[1] T. Alpcan and T. Basar, "A game theoretic application to decision and analysis in Network Intrusion Detection", 42nd IEEE CDC 2003, pp. 2595-2600, Maui, Hawaii, USA

[2] A. Agah, S. K. Das and K. Basu, "A non-cooperative game approach for intrusion detection in sensor networks", Vehicular Technology Conference, 2004. VTC2004-Fall. pp. 2902 – 2906

A Decentralized Markov Game Model

Intelligent Automation, Inc.

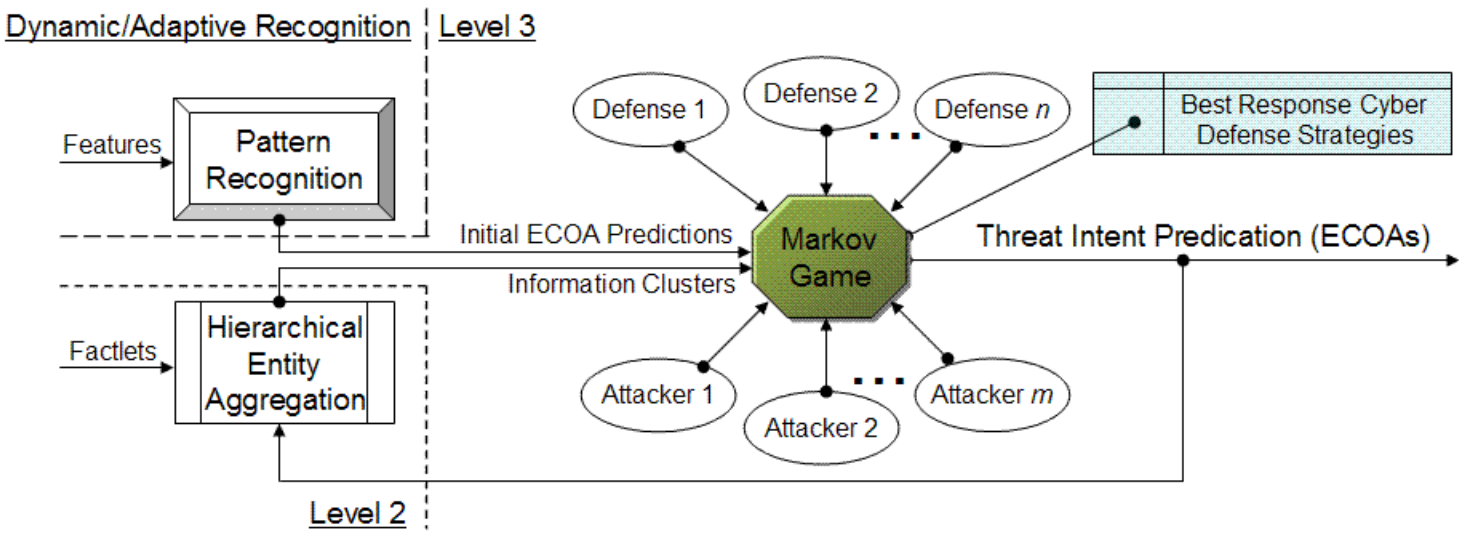
- It is not difficult to see that these matrix game models lack the sophistication to study multi-players with relatively large actions spaces, and large planning horizons.
- For the cyber decision support and attacker intent inference problem, we will revise the dynamic Markov game model[1] used for battle-space and focus on the cyber attack domain properties.
- Our approach has several features:
  - *Decentralized*. Each cluster or team of IDSs makes decisions mostly based on the local information. We put more autonomies in each group allowing for more flexibilities;
  - *Markov Decision Process* (MDP) can effectively model the uncertainties in the cyber network environment;
  - *Game framework* is an effective and ideal model to capture the nature of network conflicts;
  - *White (neutral) objects* (normal network nodes) are modeled as one of the multi-players so that their possible COA will be estimated and considered by the other players.

[1] G. Chen, D. Shen, J. B. Cruz, C. Kwan, and M. Kruger, "Game theoretic approach to threat prediction and situation awareness," ***Proceedings of 9th International Conference on Information Fusion***, Florence, Italy, 10-13 July, 2006

A Decentralized Markov Game Model

Intelligent Automation, Inc.

- Block Diagram



- In general, a Markov (stochastic) game is specified by
  - (i) a finite set of players
  - (ii) a set of states
  - (iii) for every player, a finite set of available actions
  - (iv) a transition rule
  - (v) a payoff function for each player

Player (decision maker)

- Cyber attackers, network defense system, and normal network users are players of this Markov game model.
- We denote cyber attackers as red team, network defense system (IDSs, Firewalls, Email-Filters, Encryption) as blue team, normal network user as white team.
- The cooperation within same team is also modeled so that the coordinated cyber network attacks can be captures and predicted. (Note the cooperation within a team is actually modeled by lower level cooperative games among team members, see section payoff function for details)

State Space

- All the possible states of involved network nodes consist of the state space. (It is different from the battle space model in which the COAs are system states).
- To determine the optimal IDS (intrusion detection sensor) deployment, we include the defense status for each network node in the state space.
- So for the ith network node, there is a state vector $s_i(k)$ at time k.

$$s^i(k) = (f, p, a)^T$$

where f is the working status of the ith network node, p is the protection status, and a is the status of being attacked.

- The system states are determined by two factors: 1) previous states and 2) the current actions. So the whole system can be model by a first-order Markov decision process.

Action Space

- At every time step, each player chooses targets with associated actions based on its local network information.
- The action control of the ith white player at time k is

$$u_w^i(k) = (t, v)^T$$

where vector t is the network node providing services and v is the service types requested.

- For red team (cyber network attackers), we consider the following types of network-based attacks: Buffer overflow, Semantic URL attack, E-mail Bombing, E-mail spam and Distributed Denial-of-service (DDos).
- For blue team (network defense system), we consider the following defense actions: IDS deployment, Firewall configuration , Email-filter configuration, and Shut down or reset servers

Transition Rule

- For each network node (server or workstation), the state of time $k+1$ is determined by three things:
  - state at time k;
  - control strategies of the three teams
  - the attack/defense efficiency.
- From a perceptive of battle-space control, the counterpart of attack/defense efficiency is the kill probability of weapons.
- For example, if the state of node 1 at time k is [“normal”, “NULL”, “NULL”], one component of red action is “email-bombing node 1”, one component of blue action is “email-filter –configuration-no-block for node 1”, and all white actions are not related to node 1, then the probability distribution of all possible next states of node 1 is:
  - [“normal”, “email-filter-configuration”, “email-bombing”] with probability *0.4*
  - [“slow”, “email-filter-configuration”, “email-bombing”] with probability *0.3*
  - [“crashed”, “email-filter-configuration”, “email-bombing”] with probability *0.3*.

Payoff Functions

- In our proposed decentralized Markov game model, there are two levels of payoff functions for each team (red, blue, or white):
  - Low-level (cooperative within each team)
  - High-level (non-cooperative between teams) payoff functions
  - This hierarchical structure is important to model the coordinated cyber network attacks and specify optimal coordinated network defense strategies and IDS deployment.
- The lower level payoff functions are used by each team (blue, red or white side) to determine the cooperative team actions for each team member based on the available local information.
- The top level payoff functions at time *k* are used to evaluate the overall performance of each team.
- In our approach, the lower lever payoffs are calculated distributedly by each team member and sent back to network administrator via communication networks.

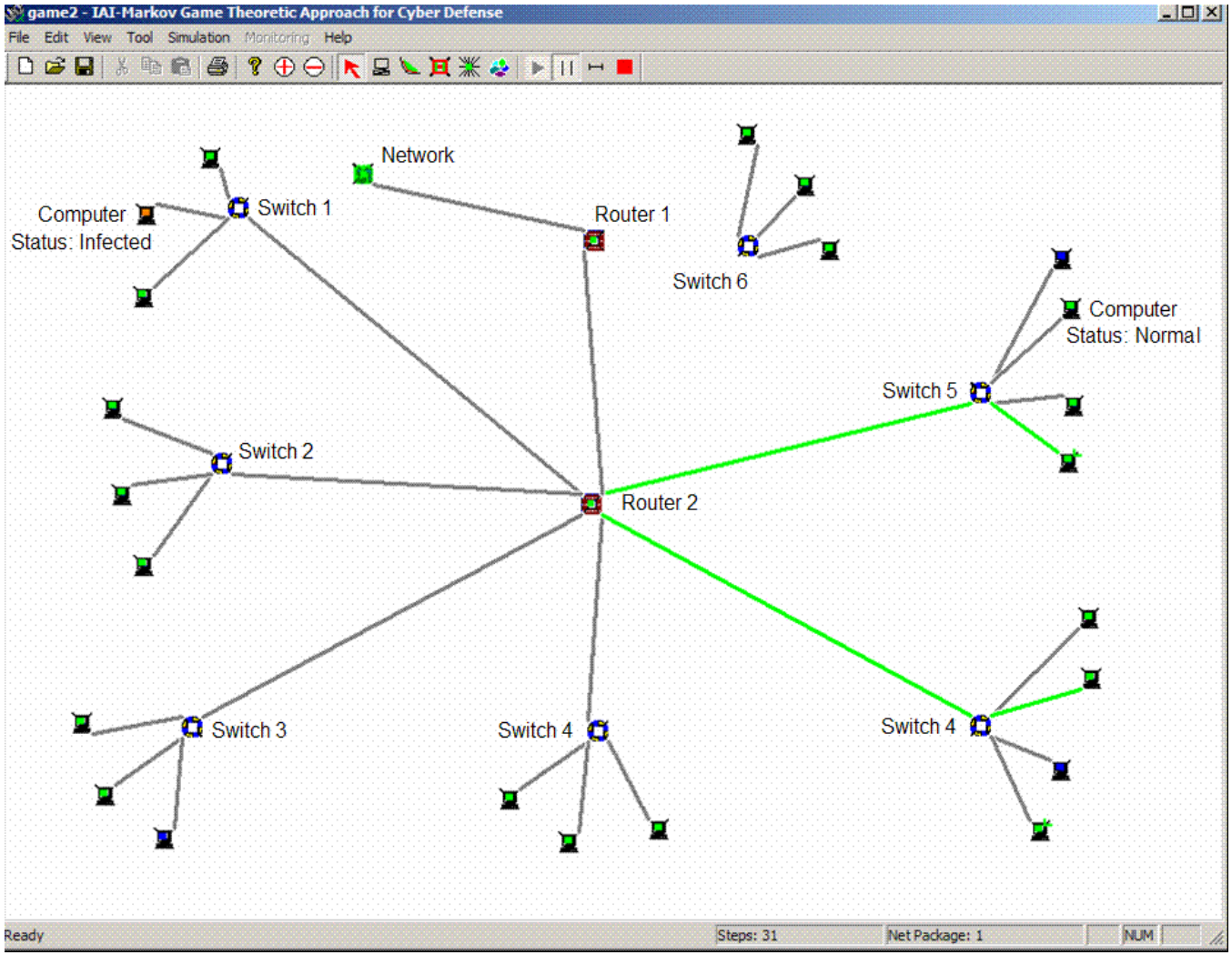
Strategies

- In game theory, the Nash equilibrium is a kind of optimal collective strategy in a game involving two or more players, where no player has anything to gain by changing only his or her own strategy.
- A mixed strategy is used in game theory to describe a strategy comprised of possible actions and an associated probability, which corresponds to how frequently the action is chosen.
- It was proved by Nash that that every finite game has Nash equilibria but not all has a pure strategy Nash equilibrium.
- In our cyber network security application, *mixed Nash strategies* are preferred since
  - the existence is guaranteed
  - the stochastic property of mixed Nash strategy is compatible to the Markov (stochastic) game model
  - Playing a mixed strategy can also keep your opponent off balance. The worst case payoff of a mixed strategy may be better than the worst case payoff of a pure strategy.

Simulations and Experiments

Intelligent Automation, Inc.

- Simulation software - Cyber Game Simulation Platform (CGSP)



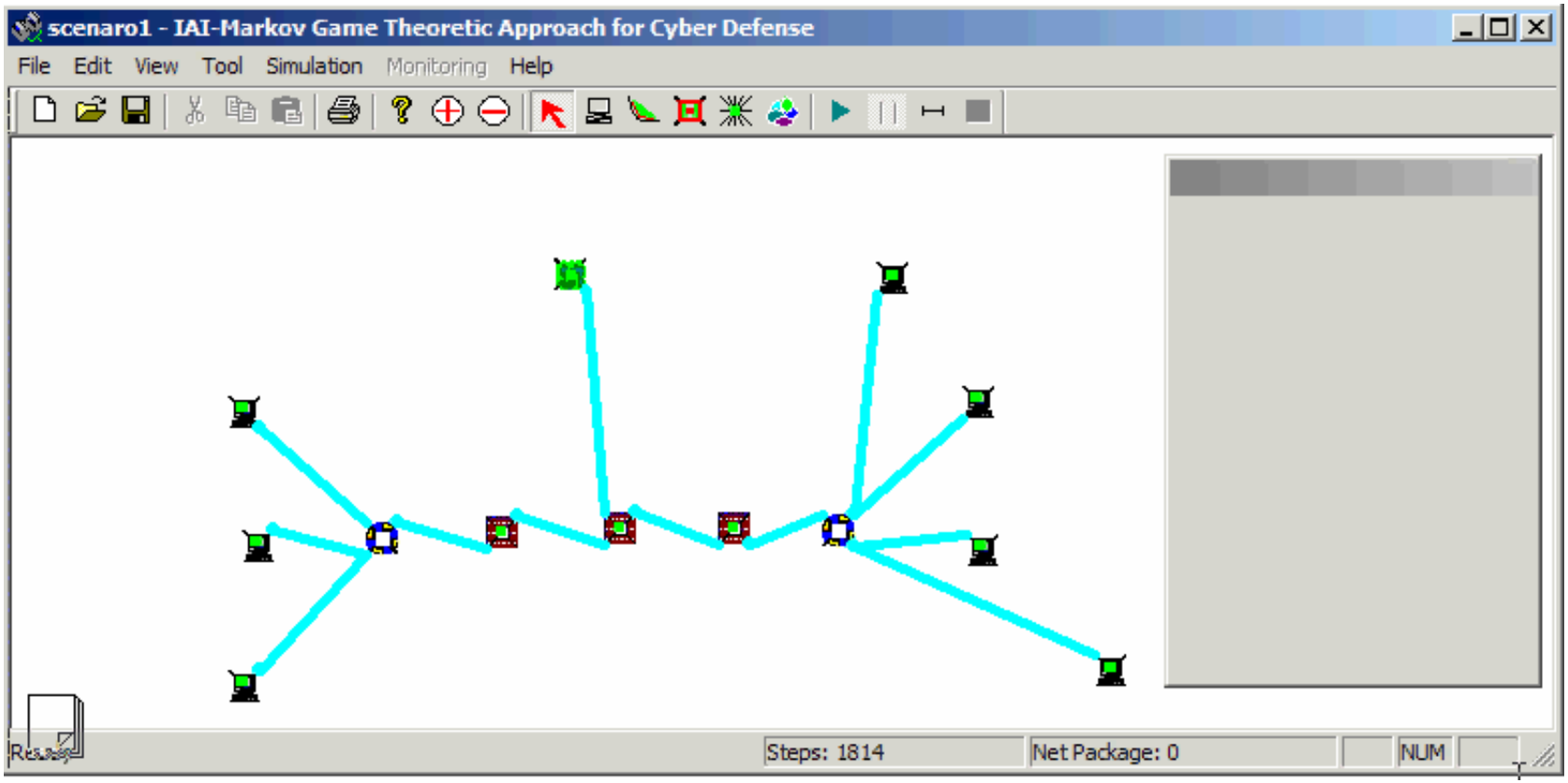
Simulations and Experiments

- Simulation software - Cyber Game Simulation Platform (CGSP)
  - The implemented network components: Computer (host), Switch, Open Shortest Path First (OSPF) Router or Firewall, Link (connection), and (Sub) Network (Simulated by a node).
  - The color of a link represents the traffic volume on that link (in KBps and in Mbps).
    - Light Gray: less than 1 percent of bandwidth
    - Green: more than 1 percent of bandwidth
    - Yellow: between green and red
    - Red: more than 30 percent of bandwidth
  - The color of a host indicates the host status.
    - Red: Infected node.
    - Green: Vulnerable node but not infected
    - Gray: Non-vulnerable node

Scenario 1 – “reset” enabled

Intelligent Automation, Inc.

- There are 7 computers, 3 routers, 2 switches, and 1 normal outside network.

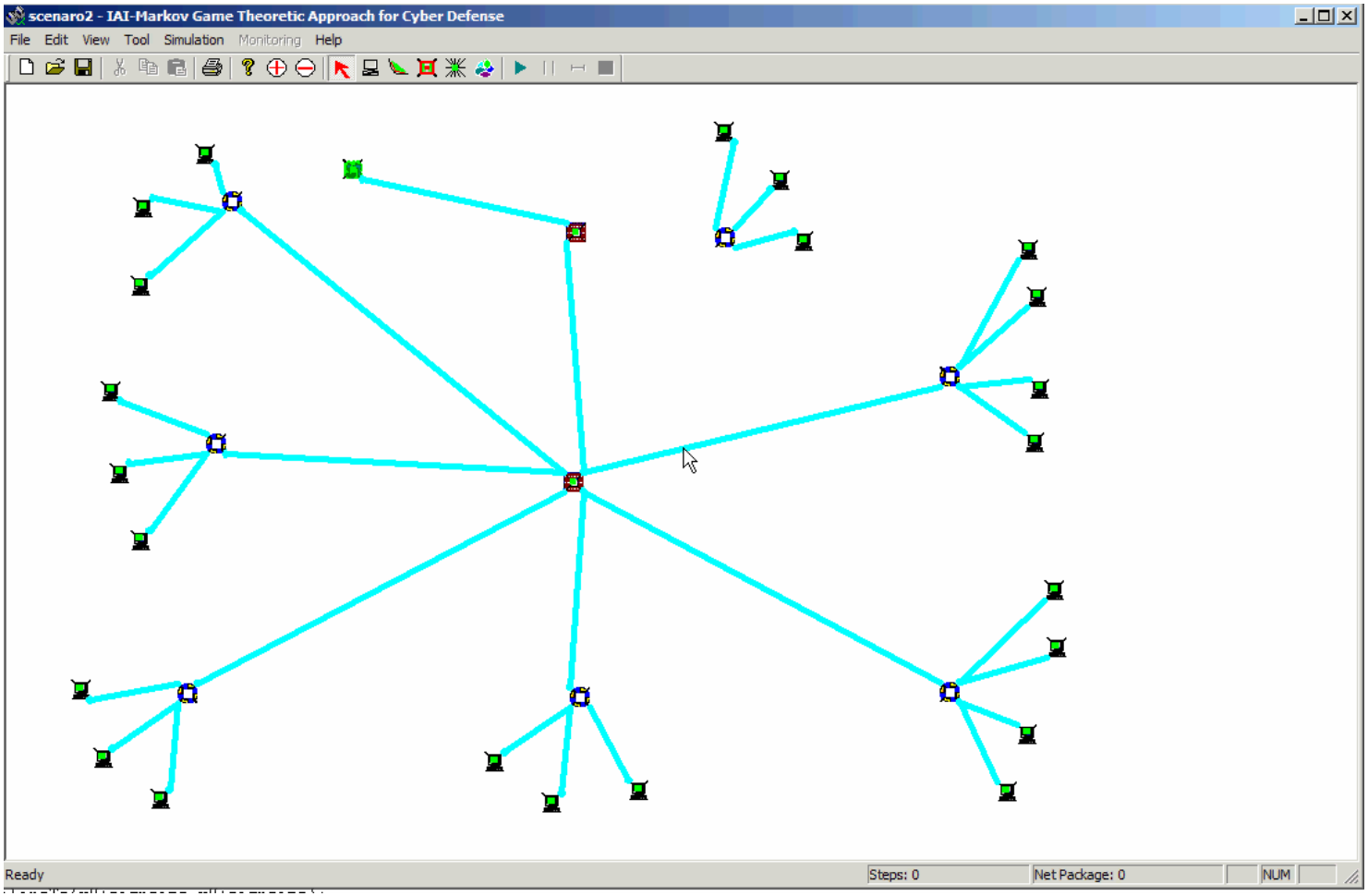


Since the network defense side can reset the computers anytime, we can see from the simulation that no servers or target computers are infected or hacked.

Scenario 2– “reset” disabled

Intelligent Automation, Inc.

- There are 23 computers, 2 routers, 7 switches, and 1 network.

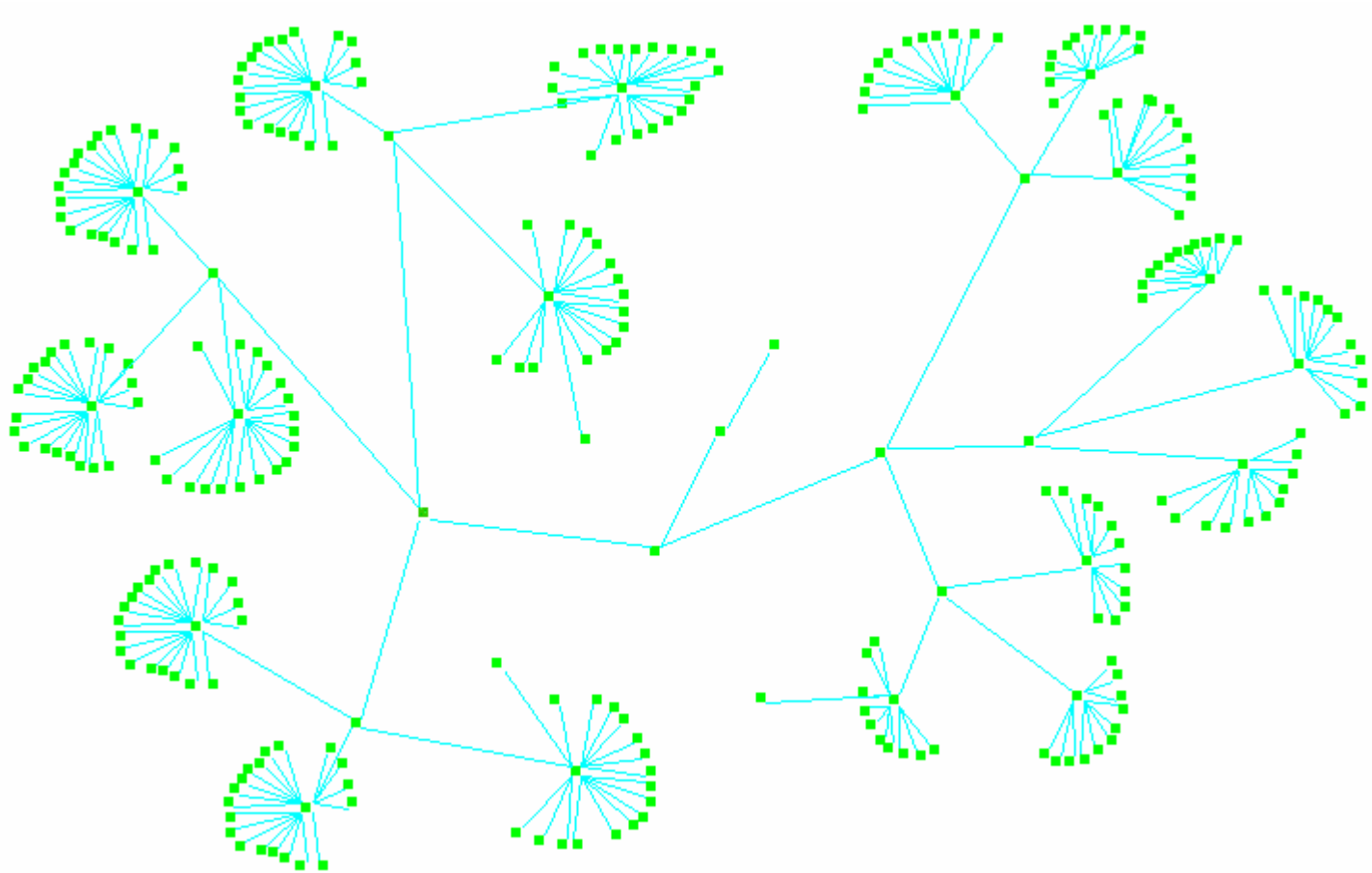


a target computer (web server) is infected or hacked. Then the computer (web server) will be used by attacking force to infect other more important target computers such as file servers or email servers.

Scenario 3– scalability test

Intelligent Automation, Inc.

- There are 269 computers, 10 routers, and 18 switches.



We can see that the simulation is slower than the previous two scenarios due to the increased computing work. Fortunately, the intelligent interactions between two sides are well simulated and demonstrated based on our Markov game model.

Conclusions

- The network security system was evaluated and protected from a perspective of data fusion and adaptive control.
- The goal of our approach was to examine the estimation of network states and projection of attack activities (similar to ECOA in the warfare scenario).
- We used Markov game theory's ability to "step ahead" to infer possible adversary attack patterns.
- Extensive simulations were performed to verify and illustrate the benefits of this model.
- Game theoretic tools have a potential for threat prediction that takes real uncertainties in red plans and deception possibilities into consideration.